

CAUCHY-DAVENPORT TYPE INEQUALITIES, I

SALVATORE TRINGALI

ABSTRACT. Let $\mathbb{G} = (G, +)$ be a group (either abelian or not). Given $X, Y \subseteq G$, we denote by $\langle Y \rangle$ the subsemigroup of \mathbb{G} generated by Y , and we set

$$\gamma(Y) := \sup_{y_0 \in Y} \inf_{y_0 \neq y \in Y} \text{ord}(y - y_0)$$

if $|Y| \geq 2$ and $\gamma(Y) := |Y|$ otherwise. We prove that if $\langle Y \rangle$ is commutative, Y is non-empty, and $X + 2Y \neq X + Y + y$ for some $y \in Y$, then

$$|X + Y| \geq |X| + \min(\gamma(Y), |Y| - 1).$$

Actually, this is obtained from a more general result, which improves on previous work of the author on sumsets in cancellative semigroups, and yields a comprehensive generalization, and in some cases a considerable strengthening, of various additive theorems, notably including the Chowla-Pillai theorem (on sumsets in finite cyclic groups) and the specialization to abelian groups of the Hamidoune-Shatrowsky theorem.

1. INTRODUCTION

Let $\mathbb{A} = (A, +)$ be, unless otherwise specified, an additively written semigroup, viz. an ordered pair consisting of a set and a binary associative operation on it; note that, in this paper, “additive” does not imply “commutative”. We address the reader to [6, § 1.1] for basic aspects of semigroup theory.

If $X_1, \dots, X_n \subseteq A$, we let $X_1 + \dots + X_n$ denote, as usual, the sumset, relative to \mathbb{A} , of the n -tuple (X_1, \dots, X_n) , namely

$$X_1 + \dots + X_n := \{x_1 + \dots + x_n : x_1 \in X_1, \dots, x_n \in X_n\};$$

we replace X_i with x_i in this notation if $X_i = \{x_i\}$ for some i , provided it does not cause confusion, and we use nX_1 for $X_1 + \dots + X_n$ if $X_1 = \dots = X_n$.

We write \mathbb{A}^\times for the set of units (or invertible elements) of \mathbb{A} , and for $X \subseteq A$ we set $X^\times := X \cap \mathbb{A}^\times$ when there is no danger of ambiguity.

2010 *Mathematics Subject Classification.* Primary 05E15, 11B13, 20D60; Secondary 20E99.

Key words and phrases. Additive theory, Cauchy-Davenport type inequalities, Chowla-Pillai theorem, Hamidoune-Shatrowski theorem, sumsets.

In particular, $A^\times = A$ if and only if \mathbb{A} is a group or A is empty, and $A^\times \neq \emptyset$ if and only if \mathbb{A} is a monoid, i.e. there exists a (provably unique) element $0_{\mathbb{A}} \in A$, labeled as the identity of \mathbb{A} , such that $x + 0_{\mathbb{A}} = 0_{\mathbb{A}} + x = x$ for all $x \in A$.

For $X, Y \subseteq A$ we let $X - Y := \{z \in A : X \cap (z + Y) \neq \emptyset\}$ and $-Y + X := \{z \in A : X \cap (Y + z) \neq \emptyset\}$, which extends the notion of difference set from groups to semigroups, at the cost that $X - Y$ or $-Y + X$ may be empty even if X and Y are not. We use, respectively, $X - y$ and $-y + X$ in place of $X - Y$ and $-Y + X$ if $Y = \{y\}$ and no confusion can arise; note that $X - y = \{x + (-y) : x \in X\}$ if $y \in A^\times$, and similarly for $-y + X$.

Given $X \subseteq A$, we denote by $\langle X \rangle$ the smallest subsemigroup of \mathbb{A} containing X , and we set $\langle\langle X \rangle\rangle := \langle X \cup \{-x : x \in X^\times\} \rangle$ and $\text{ord}(X) := |\langle X \rangle|$. If $X = \{x\}$ and there is no risk of misunderstanding, we just write $\text{ord}(x)$ in place of $\text{ord}(X)$, and we use $\langle x \rangle$ in an analogous way.

Lastly, we say that an element $z \in A$ is cancellable (in \mathbb{A}) if both the functions $A \rightarrow A : x \mapsto x + z$ and $A \rightarrow A : x \mapsto z + x$ are injective, and we refer to \mathbb{A} as a cancellative semigroup if every $z \in A$ is cancellable.

2. THE CAUCHY-DAVENPORT CONSTANT OF AN n -TUPLE

With the above in mind, we now introduce a quantity that happens to capture, as discussed below, interesting features of the “combinatorial structure” of \mathbb{A} .

To start with, we set, for every $X \subseteq A$, $\gamma(X) := |X|$ if $|X| \leq 1$, otherwise

$$\gamma(X) := \sup_{x_0 \in X^\times} \inf_{x_0 \neq x \in X} \text{ord}(x - x_0), \quad (1)$$

where $\sup(\emptyset) := 0$ and $\inf(\emptyset) := \infty$; note that (1) can be slightly simplified if \mathbb{A} is a group, by replacing X^\times with X .

Throughout, we will see how to use $\gamma(X)$ to obtain, for $X, Y \subseteq A$, non-trivial lower bounds on $|X + Y|$. But first, for all $X_1, \dots, X_n \subseteq A$ let

$$\gamma(X_1, \dots, X_n) := \begin{cases} 0 & \text{if } X_i = \emptyset \text{ for some } i; \\ \max_{1 \leq i \leq n} \gamma(X_i) & \text{otherwise} \end{cases};$$

we refer to $\gamma(X_1, \dots, X_n)$ as the *Cauchy-Davenport constant*, relative to \mathbb{A} , of the n -tuple (X_1, \dots, X_n) . Occasionally, we may add a subscript ‘ \mathbb{A} ’ to the right of the letter γ in the above definitions if we need, for any reason, to be explicit about the semigroup on which they do actually depend.

The Cauchy-Davenport constant of a tuple was first introduced in [10], though in a different notation and in a somewhat different form, and further investigated in [11], as part of a broader program aimed at the extension of aspects of the theory on Cauchy-Davenport type inequalities from groups to more abstract settings, where certain properties (of groups) are no longer necessarily true.

In particular, the author proposed in [11] to prove (or disprove) the following:

Conjecture 1. *If \mathbb{A} is a cancellative semigroup and $X_1, \dots, X_n \subseteq A$, then*

$$|X_1 + \dots + X_n| \geq \min(\gamma(X_1, \dots, X_n), |X_1| + \dots + |X_n| + 1 - n).$$

This is plainly true if $n = 1$ or $X_1^\times = \dots = X_n^\times = \emptyset$, is straightforward when $|X_i| \geq \gamma(X_1, \dots, X_n)$, and especially $|X_i| = \infty$, for some $i = 1, \dots, n$ (see Lemma 7(ii) below), and has been so far confirmed in a couple more of cases:

- (i) if $n = 2$ and each of X_1 and X_2 generates a commutative subsemigroup of \mathbb{A} , see [10, Theorem 8 and Corollary 10];
- (ii) if $\gamma(X_1) = \dots = \gamma(X_n)$ and \mathbb{A} is commutative (in addition to being cancellative), see the note added in proof at the end of [11, § 6].

The conjecture was first motivated by point (i) above and the following theorem, see [11, Theorem 7]: if \mathbb{A} is a cancellative semigroup and $X, Y \subseteq A$, then

$$|X + Y| \geq \min(\gamma(X + Y), |X| + |Y| - 1). \quad (2)$$

In fact, (2) is weaker than the bound provided by Conjecture 1 in the case of two summands, as $\gamma(X, Y) \geq \gamma(X + Y)$ in general, and actually $\gamma(X, Y) \gg \gamma(X + Y)$ in many common situations, see [11, Lemma 3 and Example 4]. (The symbol ‘ \gg ’ means that, for a suitable choice of the semigroup \mathbb{A} and the sets X and Y , the left-hand side can be made larger than the right-hand side by an arbitrary factor.)

With all this said, here comes the main contribution of the present work, which is, in the first place, a strengthening of the Cauchy-Davenport theorem [1, 3, 4].

Theorem 2. *Assume \mathbb{A} is a cancellative semigroup, and let $X, Y \subseteq A$ such that $\langle Y \rangle$ is commutative and $Y \neq \emptyset$. Then at least one of the following holds:*

- (i) $|X + Y| \geq |X| + \min(\gamma(Y), |Y| - 1)$;
- (ii) $X + 2Y = X + Y + \bar{y}$ for some $\bar{y} \in Y^\times$.

Loosely speaking, the theorem says that, for all $X, Y \subseteq A$, and in the presence of cancellativity, $|X + Y|$ cannot be “too small”, unless $X + Y$ has “structure”, which is made more precise by the next statement, whose proof we defer to the end of § 3.

Proposition 3. *Assume \mathbb{A} is a cancellative semigroup, and let $X, Y \subseteq A$ be finite sets such that $\langle Y \rangle$ is commutative and $Y^\times \neq \emptyset$. Then the following are equivalent:*

- (i) $X + 2Y = X + Y + \bar{y}$ for some $\bar{y} \in Y^\times$;
- (ii) $X + 2Y = X + Y + y$ for all $y \in Y$;
- (iii) $X + \langle\langle Y - \bar{y} \rangle\rangle = X + \langle Y - \bar{y} \rangle = X + Y - \bar{y}$ for every $\bar{y} \in Y^\times$.

We use Theorem 2 and Proposition 3 to prove a couple of corollaries: the first has essentially the same content of [10, Theorem 8], and deriving it from Theorem 2 shows, in the end, that the results of this paper subsume and strengthen

all those obtained in [10]; the second is reminiscent of an addition theorem of Y. O. Hamidoune [5, p. 249] we refer to as the Hamidoune-Shatrowsky theorem, as it is a generalization of an earlier (and weaker) result of L. Shatrowsky [9].

Corollary 4. *Assume \mathbb{A} is a cancellative semigroup, and let $X, Y \subseteq A$ such that $X \neq \emptyset$ and $\langle Y \rangle$ is commutative. Then $|X + Y| \geq \min(\gamma(Y), |X| + |Y| - 1)$.*

Corollary 5. *Let \mathbb{A} be a cancellative monoid with identity $0_{\mathbb{A}}$, and let $X, Y \subseteq A$ such that $\langle Y \rangle$ is commutative and $X \cup (X + Y) \neq X + \langle Y \rangle$. Then*

$$|X \cup (X + Y)| \geq |X| + \min(\gamma(Y \cup \{0_{\mathbb{A}}\}), |Y| - \mathbf{1}_Y(0_{\mathbb{A}})), \quad (3)$$

where $\mathbf{1}_Y(0_{\mathbb{A}}) := 1$ if $0_{\mathbb{A}} \in Y$, otherwise $\mathbf{1}_Y(0_{\mathbb{A}}) := 0$.

As long as $\langle Y \rangle$ is commutative, Corollary 5 is indeed stronger, and can be *much* stronger, than the Hamidoune-Shatrowsky theorem, according to which we would rather have that if \mathbb{A} is a group, $Y \neq \emptyset$, and $X \cup (X + Y) \neq X + \langle Y \rangle$, then

$$|X \cup (X + Y)| \geq |X| + \min(v(Y), |Y|), \quad (4)$$

where $v(Y)$ is the minimal order of the elements of Y . In fact, there are two cases:

- (i) $0_{\mathbb{A}} \in Y$. Then $X \subseteq X + Y$ and $v(Y) = 1$, hence (4) simplifies to $|X + Y| \geq |X| + 1$. If $|Y| \geq 2$, this is (strictly) weaker than (3), and actually *much* weaker than (3) for (comparatively) large values of both $\gamma(Y \cup \{0_{\mathbb{A}}\})$ and $|Y|$ (which can be easily attained). Otherwise, $Y = \{0_{\mathbb{A}}\}$ and $X + \langle Y \rangle = X + Y = X$, which, however, would be a contradiction.
- (ii) $0_{\mathbb{A}} \notin Y$. Then $|Y| - \mathbf{1}_Y(0_{\mathbb{A}}) = |Y|$, and of course $\gamma(Y \cup \{0_{\mathbb{A}}\}) \geq v(Y)$.

On the other hand, the Hamidoune-Shatrowsky theorem holds, provided \mathbb{A} is a group, without the additional assumption on $\langle Y \rangle$ made in Corollary 5, which leads us to believe that a more general version of Theorem 2 should be true.

Incidentally, let us mention here that, while the original proof of the Hamidoune-Shatrowsky theorem relies on Hamidoune's theory of atoms, our proof of Theorem 2, and hence of Corollary 5, is essentially based on a non-commutative variant of the Davenport transform first considered, to our knowledge, in [10, § 4].

Our last result is a special case of Theorem 2 and a strengthening of [10, Corollary 15], which is in turn a generalization of the Chowla-Pillai theorem (on sumsets in finite cyclic groups), see [2, Theorem 1] and [8, Theorems 1–3].

Corollary 6. *Fix $n \in \mathbf{N}^+$. Denote by $(\mathbf{Z}_n, +)$ the additive group of the integers modulo n and by π the canonical projection $\mathbf{Z} \rightarrow \mathbf{Z}_n$. Let $X, Y \subseteq \mathbf{Z}_n$ be non-empty sets such that $X + 2Y \neq X + Y + \bar{y}$ for some $\bar{y} \in Y$. Then*

$$|X + Y| \geq |X| + \min(\delta_Y^{-1}n, |X| + |Y| - 1),$$

where $\delta_Y := 1$ if $|Y| = 1$, otherwise

$$\delta_Y := \min_{y_0 \in \pi^{-1}(Y)} \max_{y \in \pi^{-1}(Y), \pi(y) \neq \pi(y_0)} \gcd(n, y - y_0).$$

We will prove Theorem 2 and its corollaries in § 4, but first we need to gather together a few facts that play a role in the proofs: this is done in the next section.

3. PREPARATIONS

We start with basic properties of semigroups that are readily adapted from the case of groups and used repeatedly in the sequel (with or without a comment).

Lemma 7. *The following hold:*

- (i) *If $z \in A$ is cancellable and $X \subseteq A$, then $|z + X| = |X + z| = |X|$.*
- (ii) *If $X_1, \dots, X_n \subseteq A$ and X_i contains at least one cancellable element for each i , then $|X_1 + \dots + X_n| \geq \max_{1 \leq i \leq n} |X_i|$.*
- (iii) *Let $z \in A$, and assume z is cancellable and $n := \text{ord}(z) < \infty$. Then \mathbb{A} is a monoid and nz is the identity of \mathbb{A} .*
- (iv) *Let \mathbb{A} be a monoid and $X \subseteq A$, and let $z \in \mathcal{C}(X) \cap A^\times$, where*

$$\mathcal{C}(X) := \{z \in A : x + z = z + x \text{ for all } x \in X\}$$

is the center of X (in \mathbb{A}). Then $-z \in \mathcal{C}(X)$, and $\langle X - z \rangle$ and $\langle -z + X \rangle$ are both commutative subsemigroups if $\langle X \rangle$ is.

Proof. (i)–(ii) Units are cancellable elements, and for a cancellable $z \in A$ both the functions $A \rightarrow A : x \mapsto x + z$ and $A \rightarrow A : x \mapsto z + x$ are injective.

(iii) By hypothesis, $(n + 1)z = kz$ for some $k = 1, \dots, n$. We claim that $k = 1$. Indeed, if $k \geq 2$ then z being cancellable (in \mathbb{A}) implies $(n + 2 - k)z = z$, which is impossible, since $2 \leq n + 2 - k \leq n$ and z, \dots, nz are pairwise distinct.

So, for all $x \in A$ we have $x + z = (x + nz) + z$ and $z + (nz + x) = z + x$, which, by using again that z is cancellable, yields $x + nz = nz + x = x$, and ultimately means that \mathbb{A} is a monoid with identity nz .

(iv) Let $z \in \mathcal{C}(X)$ and $x \in X$, and for ease of notation denote by \tilde{z} the inverse of z . By the cancellativity of \mathbb{A} , it is immediate that $x + \tilde{z} = \tilde{z} + x$ if and only if $x = (x + \tilde{z}) + z = \tilde{z} + x + z$, which is true, as $\tilde{z} + x + z = \tilde{z} + z + x = x$ by the assumptions on x and z . It follows that $\tilde{z} \in \mathcal{C}(X)$.

With this in hand, suppose $\langle X \rangle$ is a commutative subsemigroup of \mathbb{A} and pick $v, w \in \langle X - z \rangle$. Then, there exist $k, \ell \in \mathbf{N}^+$ and $x_1, \dots, x_k, y_1, \dots, y_\ell \in X$ such that $v = \sum_{i=1}^k (x_i + \tilde{z})$ and $w = \sum_{i=1}^\ell (y_i + \tilde{z})$, with the result that $v + w = w + v$ by induction on $k + \ell$ and the observation that, for all $u_1, u_2 \in X$, it holds

$$(u_1 + \tilde{z}) + (u_2 + \tilde{z}) = u_1 + u_2 + 2\tilde{z} = u_2 + u_1 + 2\tilde{z} = (u_2 + \tilde{z}) + (u_1 + \tilde{z}),$$

where we have used, in particular, that $\tilde{z} \in \mathcal{C}(X)$, as proved in the above. Hence $\langle X - z \rangle$ also is commutative, and the case of $\langle -z + X \rangle$ is analogous. \blacksquare

We omit the proof of the next elementary lemma, but the interested reader can refer to [11, Lemma 12 and Remark 13] for details.

Lemma 8. *If $X_1, \dots, X_n \subseteq A$, then $X_1^\times + \dots + X_n^\times \subseteq (X_1 + \dots + X_n)^\times$, and the inclusion is actually an equality provided that \mathbb{A} is cancellative.*

Moreover, if \mathbb{A} is a monoid and $x_1 \in X_1^\times, \dots, x_n \in X_n^\times$, then $x := x_1 + \dots + x_n$ is too an invertible element and $-x = (-x_n) + \dots + (-x_1)$.

The following result reveals a certain invariance of the Cauchy-Davenport constant; we address the reader to [11, Proposition 14] for a proof.

Lemma 9. *Assume \mathbb{A} is a monoid, and let $X \subseteq A$ and $z \in A^\times$. Then*

$$\gamma(X) = \gamma(X - z) = \gamma(-z + X).$$

Given $X, Y \subseteq A$, we say that a pair (X_0, Y_0) of subsets of A is an invariant transform, relative to \mathbb{A} , of (X, Y) if:

- (s1) $|X + Y| = |X_0 + Y_0|$;
- (s2) $|X| = |X_0|$ and $|Y| = |Y_0|$;
- (s3) $\gamma(X) = \gamma(X_0)$ and $\gamma(Y) = \gamma(Y_0)$.

This notion is motivated by the next lemma, cf. [11, Corollary 15].

Lemma 10. *Let \mathbb{A} be a cancellative monoid with identity $0_{\mathbb{A}}$, and pick $X, Y \subseteq A$. Assume that $Y^\times \neq \emptyset$ and $|Y| \geq 2$, and let κ be an integer $\leq \gamma(Y)$. Then, there exists an invariant transform (X_0, Y_0) of (X, Y) such that:*

- (i) $0_{\mathbb{A}} \in Y_0$ and $\gamma(Y_0) \geq \text{ord}(y) \geq \kappa$ for every $y \in Y_0 \setminus \{0_{\mathbb{A}}\}$;
- (ii) if $\langle Y \rangle$ is commutative, then so is $\langle Y_0 \rangle$;
- (iii) if $\langle Y \rangle$ is commutative and $X + 2Y \neq X + Y + \bar{y}$ for every $\bar{y} \in Y^\times$, then $X_0 + 2Y_0 \neq X_0 + Y_0 + \bar{y}_0$ for all $\bar{y}_0 \in Y_0^\times$.

Proof. Fix an integer $\kappa \leq \gamma(Y)$, and using that $Y^\times \neq \emptyset$ and $|Y| \geq 2$, let $y_0 \in Y^\times$ such that $\gamma(Y) \geq \inf_{y_0 \neq y \in Y} \text{ord}(y - y_0) \geq \kappa$. Then, set

$$X_0 := X + y_0 \quad \text{and} \quad Y_0 := -y_0 + Y.$$

Clearly, $0_{\mathbb{A}}$ is in Y_0 , and a straightforward computation gives that

$$X + Y = (X + y_0) + (-y_0 + Y) = X_0 + Y_0. \tag{5}$$

In addition, since $y_0 \in A^\times$ and units are cancellable, we have from Lemma 9 that $\gamma(X) = \gamma(X_0)$ and $\gamma(Y) = \gamma(Y_0)$, and from Lemma 7(i) that $|X| = |X_0|$ and

$|Y| = |Y_0|$. Lastly, using that $0_{\mathbb{A}} \in Y_0$ and, on the other hand, $v \in Y_0$ if and only if $v = y - y_0$ for some $y \in Y$, we find

$$\gamma(Y_0) \geq \inf_{0_{\mathbb{A}} \neq v \in Y_0} \text{ord}(v) = \inf_{y_0 \neq y \in Y} \text{ord}(y - y_0) \geq \kappa.$$

Putting it all together, this shows that (X_0, Y_0) is an invariant transform of (X, Y) . So point (i) is proved, and (ii) follows from Lemma 7(iv).

As for (iii), suppose that $\langle Y \rangle$ is commutative and $X + 2Y \neq X + Y + \bar{y}$ for all $\bar{y} \in \langle Y \rangle$, yet $X_0 + 2Y_0 = X_0 + Y_0 + \bar{v}$ for some $\bar{v} \in Y_0^\times$. Accordingly, note that $Y_0^\times = -y_0 + Y^\times$ by Lemma 8, and let $\bar{y} \in Y^\times$ such that $\bar{v} = -y_0 + \bar{y}$. Then, we get from (5) and point (ii) above that

$$X + Y + \bar{y} - y_0 = X_0 + 2Y_0 = X + 2Y - y_0,$$

which yields $X + 2Y = X + Y + \bar{y}$ (again, because $-y_0$ is a unit, and hence we can cancel it out). This, however, is absurd and leads to the desired conclusion. \blacksquare

Last but not least, we will need the following proposition, which is essentially a revised version of [10, Proposition 23].

Proposition 11. *Assume \mathbb{A} is a cancellative semigroup, and let $X, Y \subseteq A$ be such that $X + 2Y \not\subseteq X + Y$ and $\langle Y \rangle$ is a commutative subsemigroup of \mathbb{A} . Accordingly, fix $z \in (X + 2Y) \setminus (X + Y) \neq \emptyset$, and define*

$$\tilde{Y}_z := \{y \in Y : z \in X + Y + y\} \quad \text{and} \quad Y_z := Y \setminus \tilde{Y}_z. \quad (6)$$

Then the following hold:

- (i) $(X + Y_z) \cup (z - \tilde{Y}_z) \subseteq X + Y$;
- (ii) $(X + Y_z) \cap (z - \tilde{Y}_z) = \emptyset$;
- (iii) $|z - \tilde{Y}_z| \geq |\tilde{Y}_z|$;
- (iv) $|X + Y| + |Y_z| \geq |X + Y_z| + |Y|$.

Proof. (i) Let $w \in z - \tilde{Y}_z$. Then, there exists $y \in \tilde{Y}_z$ such that $z = w + y$. But $y \in \tilde{Y}_z$ if and only if $z = \tilde{w} + y$ for some $\tilde{w} \in X + Y$, so $w = \tilde{w}$ by cancellativity, and hence $w \in X + Y$. This shows that $z - \tilde{Y}_z \subseteq X + Y$, and then we are done, as it is clear, on the other hand, that $X + Y_z \subseteq X + Y$.

(ii) Suppose for a contradiction that $W := (X + Y_z) \cap (z - \tilde{Y}_z)$ is non-empty, and let $w \in W$. Then $w = x + y_1$ and $z = w + y_2$ for some $x \in X$, $y_1 \in Y_z$, and $y_2 \in \tilde{Y}_z$. Since $\langle Y \rangle$ is commutative, it follows that

$$z = x + y_1 + y_2 = x + y_2 + y_1,$$

which implies by (6) that $y_1 \in \tilde{Y}_z$, because $Y_z, \tilde{Y}_z \subseteq Y$. This is, however, absurd, as Y_z and \tilde{Y}_z are obviously disjoint.

(iii) We have from (6) that for each $y \in \tilde{Y}_z$ there exists $w \in X + Y$ such that $z = w + y$, and hence $w \in z - \tilde{Y}_z$. On the other hand, \mathbb{A} being cancellative yields that $w + y_1 \neq w + y_2$ for all $w \in A$ and distinct $y_1, y_2 \in \tilde{Y}_z$. Thus, we see that there is an injection $\tilde{Y}_z \rightarrow z - \tilde{Y}_z$, with the result that $|z - \tilde{Y}_z| \geq |\tilde{Y}_z|$.

(iv) Note first that X and Y are non-empty, because otherwise we would have $(X + 2Y) \setminus (X + Y) = \emptyset$, in contrast to our assumptions.

Using that \mathbb{A} is cancellative, it follows from Lemma 7(ii) that $|X + Y| \geq |Y|$. This implies the claim if $|Y| = \infty$, so suppose from now on that Y is a finite set.

Then, the inclusion-exclusion principle and the above points (i)-(iii) give

$$|X + Y| \geq |X + Y_z| + |z - \tilde{Y}_z| \geq |X + Y_z| + |\tilde{Y}_z|.$$

But $\tilde{Y}_z = Y \setminus Y_z$ and $Y_z \subseteq Y$, so in the end $|X + Y| \geq |X + Y_z| + |Y| - |Y_z|$, and the proof is thus complete. \blacksquare

We conclude this section with the following:

Proof of Proposition 3. (i) \Rightarrow (ii). Assume that $X + 2Y = X + Y + \bar{y}$ for some $\bar{y} \in Y$, and let $y \in Y$. Then $X + Y + y \subseteq X + Y + \bar{y}$, and on the other hand, we have from Lemma 7(i) that $|X + Y + y| = |X + Y + \bar{y}|$. But since X and Y are finite, this is possible only if $X + Y + y = X + Y + \bar{y}$, and we are done.

(ii) \Rightarrow (iii). Pick $\bar{y} \in Y^\times$. By hypothesis, we have $X + 2Y = X + Y + \bar{y}$, and using that $\langle Y \rangle$ is commutative, this is equivalent to $X + 2(Y - \bar{y}) = X + Y - \bar{y}$.

It follows (by induction) that $X + n(Y - \bar{y}) = X + Y - \bar{y}$ for all $n \in \mathbb{N}^+$, and since $\langle W \rangle = \bigcup_{n \geq 1} nW$ for every $W \subseteq A$, we obtain

$$X + \langle Y - \bar{y} \rangle = X + Y - \bar{y}. \quad (7)$$

Now, the conclusion is trivial if X is empty. Otherwise, we get by points (i) and (ii) of Lemma 7, equation (7), and the assumption that X and Y are finite that

$$\text{ord}(Y - \bar{y}) \leq |X + \langle Y - \bar{y} \rangle| = |X + Y - \bar{y}| = |X + Y| \leq |X| \cdot |Y| < \infty,$$

Thus, $\text{ord}(y - \bar{y}) < \infty$ for all $y \in Y$, which, together with Lemma 7(iii), implies $\langle Y - \bar{y} \rangle = \langle\langle Y - \bar{y} \rangle\rangle$. This leads to the desired conclusion.

(iii) \Rightarrow (i). Let $\bar{y} \in Y^\times$. By hypothesis, we have $X + \langle Y - \bar{y} \rangle = X + Y - \bar{y}$. Together with the commutativity of Y , this implies

$$X + Y - \bar{y} \supseteq X + 2(Y - \bar{y}) = X + 2Y - 2\bar{y},$$

and hence $X + 2Y \subseteq X + Y + \bar{y}$, which is enough to conclude the proof (since, of course, $X + Y + \bar{y} \subseteq X + 2Y$). \blacksquare

4. PROOFS

We start with Theorem 2, whose proof is actually a “transformation proof”, extending to a non-commutative setting ideas first used by H. Davenport in [3].

In fact, the reasoning follows the same broad scheme of the proof of [10, Theorem 8], but differs from the latter in significant details.

Proof of Theorem 2. Set $\kappa := |X + Y|$ for brevity’s sake, and suppose that $X + 2Y \neq X + Y + \bar{y}$ for all $\bar{y} \in Y^\times$. We have to prove that

$$\kappa \geq |X| + \min(\gamma(Y), |Y| - 1). \quad (8)$$

This is obvious if $Y^\times = \emptyset$ or $|Y| = 1$, since in that case the right-hand side of (8) equals $|X|$, and $\kappa \geq |X|$ by Lemma 7(ii). So we assume for the sequel that Y^\times is non-empty and $|Y| \geq 2$.

Then, also X is non-empty, otherwise $X + 2Y = X + Y + \bar{y} = \emptyset$ for every unit $\bar{y} \in Y^\times$, in contrast to our hypotheses (as $Y^\times \neq \emptyset$). Hence, we are done if X or Y is infinite, since $\kappa \geq \max(|X|, |Y|)$, again by Lemma 7(ii).

Putting it all together, we are thus reduced to the case where

$$1 \leq |X| < \infty, \quad 2 \leq |Y| < \infty, \quad \text{and} \quad Y^\times \neq \emptyset, \quad (9)$$

which means, among other things, that \mathbb{A} is (necessarily) a monoid; as usual, we will denote the identity of \mathbb{A} by $0_{\mathbb{A}}$.

Building on these premises, we now suppose, towards a contradiction, that

$$\kappa < |X| + \min(\gamma(Y), |Y| - 1). \quad (10)$$

More precisely, we assume that (X, Y) is a minimal counterexample to (8), in the sense that if (\bar{X}, \bar{Y}) is another pair of non-empty subsets of A such that $\langle \bar{Y} \rangle$ is commutative, $|\bar{Y}| \geq 2$ and $\bar{X} + 2\bar{Y} \neq \bar{X} + \bar{Y} + \bar{y}$ for every $\bar{y} \in \bar{Y}^\times$, and

$$|\bar{X} + \bar{Y}| < |\bar{X}| + \min(\gamma(\bar{Y}), |\bar{Y}| - 1),$$

then $|Y| \leq |\bar{Y}|$; of course, this is always possible and involves no loss of generality. Lastly, we may further assume, as we do, that

$$0_{\mathbb{A}} \in Y \quad \text{and} \quad \gamma(Y) \geq \inf_{0_{\mathbb{A}} \neq y \in Y} \text{ord}(y) \geq \kappa - |X| + 1, \quad (11)$$

for we get by (9), (10), and Lemma 10 that this, again, does not affect the generality of the reasoning. Accordingly, we have that

$$X + 2Y \not\subseteq X + Y.$$

In fact, $0_{\mathbb{A}} \in Y$ yields that $X + Y \subseteq X + 2Y$; therefore, $X + 2Y \subseteq X + Y$ would imply $X + 2Y = X + Y + 0_{\mathbb{A}}$, which is, however, impossible, as we are supposing $X + 2Y \neq X + Y + \bar{y}$ for every $\bar{y} \in Y^\times$.

So, let z be some element in the non-empty set $(X + 2Y) \setminus (X + Y)$, and define

$$\tilde{Y}_z := \{y \in Y : z \in X + Y + y\} \quad \text{and} \quad Y_z := Y \setminus \tilde{Y}_z.$$

Clearly, $\tilde{Y}_z \neq \emptyset$ and $0_{\mathbb{A}} \notin \tilde{Y}_z$, so we have by (11) that $0_{\mathbb{A}} \in Y_z$ and $1 \leq |Y_z| < |Y|$. Then, exploiting that $\langle Y \rangle$ is commutative and $|Y| < \infty$, we obtain by Proposition 11(iv) and equation (10) that

$$|X + Y_z| \leq |X + Y| + |Y_z| - |Y| < |X| + |Y_z| - 1. \quad (12)$$

It follows that $|Y_z| \geq 2$, as otherwise we would have from Lemma 7(i) and (12) that $|X| = |X + Y_z| < |X|$, which is absurd. To summarize, we have found that

$$0_{\mathbb{A}} \in Y_z \subsetneq Y, \quad 2 \leq |Y_z| < |Y|, \quad \text{and} \quad |X + Y_z| < |X| + |Y_z| - 1, \quad (13)$$

which, along with (10) and (11), gives

$$|X + Y_z| \leq \kappa < |X| + \inf_{0_{\mathbb{A}} \neq y \in Y} \text{ord}(y) \leq |X| + \inf_{0_{\mathbb{A}} \neq y \in Y_z} \text{ord}(y) \leq |X| + \gamma(Y_z), \quad (14)$$

where we have used, in particular, that $|Y_z| \geq 2$ and $Y_z^\times \neq \emptyset$ by (13), and that $\inf(C) \leq \inf(B)$ provided $\emptyset \neq B \subseteq C \subseteq \mathbb{N} \cup \{\infty\}$.

This is, however, absurd, as (13) and (14) together contradict the minimality of the pair (X, Y) , and it concludes the proof. \blacksquare

Now we can proceed to prove the corollaries of Theorem 2.

Proof of Corollary 4. The claim is trivial if $|X + Y| \geq |X| + \min(\gamma(Y), |Y| - 1)$, or $|Y| \leq 1$, or Y^\times is empty. Otherwise, we have from Theorem 2 and Proposition 3(iii) that $X + Y - \bar{y} = X + \langle Y - \bar{y} \rangle$ for some $\bar{y} \in Y^\times$. Consequently, points (i) and (ii) of Lemma 7, along with Lemma 8, give that

$$|X + Y| = |X + Y - \bar{y}| \geq |\langle Y - \bar{y} \rangle| \geq \text{ord}((y - \bar{y}) - (y_0 - \bar{y})) = \text{ord}(y - y_0)$$

for all $y \in Y$ and $y_0 \in Y^\times$, and this yields $|X + Y| \geq \gamma(Y)$. \blacksquare

Proof of Corollary 5. Of course, X is non-empty, otherwise $X \cup (X + Y) = X + \langle Y \rangle$. Consequently, the claim is trivial if X and Y is infinite, since in that case $|X \cup (X + Y)| = \infty$ by Lemma 7(ii), and it is still trivial if Y is empty, since then either side of equation (4) is equal to $|X|$.

So, we assume for the sequel that X and Y are both finite and non-empty, in such a way that $X \cup (X + Y)$ is finite too, and set $Y_0 := Y \cup \{0_{\mathbb{A}}\}$.

We claim that $X + Y_0 = X \cup (X + Y) \neq X + \langle Y_0 \rangle$. If $\langle Y \rangle$ is infinite, this is clear from the above; otherwise, $\langle Y_0 \rangle = \langle Y \rangle$ by Lemma 7(iii), and we have (by hypothesis) $X \cup (X + Y) \neq X + \langle Y \rangle$.

Therefore, we get from Theorem 2 and Proposition 3(iii) that

$$|X \cup (X + Y)| = |X + Y_0| \geq |X| + \min(\gamma(Y_0), |Y_0| - 1),$$

which concludes the proof, because $|Y_0| - 1 = |Y| - \mathbf{1}_Y(0_{\mathbb{A}})$. \blacksquare

Proof of Corollary 6. To begin, let \tilde{w} denote, for every $w \in \mathbf{Z}_n$, the smallest non-negative integer in w . The claim is trivial if Y is a singleton. Otherwise, since $\text{ord}(w - w_0) = n / \gcd(n, \tilde{w} - \tilde{w}_0)$ for all $w, w_0 \in \mathbf{Z}_n$, we have

$$\gamma(Y) = \max_{y_0 \in Y} \min_{y_0 \neq y \in Y} \text{ord}(y - y_0) = \frac{n}{\min_{y_0 \in Y} \max_{y_0 \neq y \in Y} \gcd(n, \tilde{y} - \tilde{y}_0)}.$$

It follows that $\gamma(Y) = \delta_Y^{-1}n$, because $\gcd(n, \tilde{y}) = \gcd(n, \xi)$ for every $y \in \mathbf{Z}_n$ and $\xi \in \mathbf{Z}$ with $\xi \equiv \tilde{y} \pmod{n}$. So we are done by Theorem 2 and Proposition 3(ii). \blacksquare

5. CLOSING REMARKS

The bound provided by Theorem 2(i) is meaningful only if $\gamma(X) > 0$, insofar as \mathbb{A} being a cancellative semigroup implies, by Lemma 7(ii), that $|X + Y| \geq |X|$. This means, in particular, that the theorem is not very useful unless \mathbb{A} is a monoid, and raises the challenge of further generalizing the result (and its corollaries) so as to replace X^\times in (1) with a subset of A that is significant also when $A^\times = \emptyset$.

On a similar note, every *commutative* cancellative semigroup can be embedded into a group. It was, however, proved by A. Malcev in [7] that there are finitely generated cancellative semigroups that do *not* embed into a group, which serves as a “precondition” for some aspects of the present work and its prequels [10, 11], as it shows that the study of sumsets in cancellative semigroups cannot be systematically reduced, in the absence of commutativity, to the case of groups (at least, not in an obvious way).

6. ACKNOWLEDGMENTS

This research was supported by the Austrian FWF Project M1900-N39, and partly by the French ANR Project ANR-12-BS01-0011. The author is grateful to Paolo Leonetti (Università Bocconi, Italy) for some useful comments.

REFERENCES

- [1] A. L. Cauchy, *Recherches sur les nombres*, J. École Polytech. **9** (1813), 99–116.
- [2] I. Chowla, *A Theorem on the Addition of Residue Classes: Application to the Number $\Gamma(k)$ in Waring’s Problem*, Q. J. Math. (O.S.) **8** (1937), No. 1, 99–102.
- [3] H. Davenport, *On the Addition of Residue Classes*, J. Lond. Math. Soc. **10** (1935), 30–32.
- [4] ———, *A Historical Note*, J. Lond. Math. Soc. **22** (1947), 100–101.
- [5] Y. O. Hamidoune, *A Generalization of an Addition Theorem of Shatrowsky*, European J. Combin. **13** (1992), No. 4, 249–255.
- [6] J. M. Howie, *Fundamentals of Semigroup Theory*, London Math. Soc. Monogr. Ser. (N.S.) **12**, Oxford Univ. Press, Oxford, 2003 (reprinted ed.).
- [7] A. Malcev, *On the Immersion of an Algebraic Ring into a Field*, Math. Ann. **113** (1937), No. 1, 686–691.

- [8] S. S. Pillai, *Generalization of a Theorem of Davenport on the Addition of Residue Classes*, Proc. Indian Acad. Sc. (A) **6** (1937), No. 3, 179–180.
- [9] L. Shatrowsky, *A new generalization of Davenport's-Pillai's theorem on the addition of residue classes*, Dokl. Akad. Nauk **45** (1944), 315–317.
- [10] S. Tringali, *A Cauchy-Davenport theorem for semigroups*, Unif. Distrib. Theory **9** (2014), No. 1, 27–42.
- [11] ———, *Cauchy-Davenport type theorems for semigroups*, Mathematika **62** (2016), No. 1, 1–12.

INSTITUTE FOR MATHEMATICS AND SCIENTIFIC COMPUTING, UNIVERSITY OF GRAZ —
HEINRICHSTR. 36, 8010 GRAZ, AUSTRIA

E-mail address: `salvatore.tringali@uni-graz.at`

URL: `http://143.50.47.129/tringali/home.html`